System and Organization Controls (SOC 3) Report

Report on the Enterprise Health System Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy

For the Period January 1, 2019 to January 31, 2020

B&A Behunin & Associates

Independent Service Auditor’s Report

To: Enterprise Health

Scope

We have examined Medical Informatics Engineering, Inc. dba Enterprise Health’s (“Enterprise Health”) accompanying assertion titled “Enterprise Health’s Assertion” (“assertion”) that the controls within Enterprise Health’s, Enterprise Health System (“system”) were effective throughout the period January 1, 2019, to January 31, 2020, to provide reasonable assurance that Enterprise Health’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in the TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)***.**

Service Organization’s Responsibilities

Enterprise Health is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Enterprise Health’s service commitments and system requirements were achieved. Enterprise Health has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Enterprise Health is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization’s service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements;

- Assessing the risks that controls were not effective to achieve Enterprise Health’s service commitments and system requirements based on the applicable trust services criteria; and

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Enterprise Health's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that Enterprise Health's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Enterprise Health's, Enterprise Health System, were effective throughout the period January 1, 2019, to January 31, 2020, to provide reasonable assurance that Enterprise Health's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Behunin & Associates, P.C.

Collegeville, Pennsylvania
April 8, 2020

enterprise**health**

Enterprise Health's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Enterprise Health's system (system) throughout the period January 1, 2019, to January 31, 2020, to provide reasonable assurance that Enterprise Health's service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2019, to January 31, 2020, to provide reasonable assurance that Enterprise Health's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Enterprise Health's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period January 1, 2019, to January 31, 2020, to provide reasonable assurance that Enterprise Health's service commitments and system requirements were achieved based on the applicable trust services criteria.

Enterprise Health Management

Attachment A

Note to readers: *The following description of the boundaries of the system is for illustrative purposes only and is not meant to be prescriptive. For brevity, the illustration does not include everything that might be described in a description of the boundaries of the service organization's system.*

Enterprise Health's Description of the Boundaries of Its Enterprise Health System

Overview of Operations

Company Background

Medical Informatics Engineering, Inc. (MIE) is a privately held corporation founded in 1995 to provide health information technology services to healthcare providers, consumers, and employers.

MIE aggregated two decades of clinical information management experience, digital consumer engagement expertise, interoperability know-how, and occupational health and compliance capability to develop web-based health information technology.

MIE's operating entities include Enterprise Health. The Enterprise Health IT solution combines occupational health and compliance, clinical care, and employee engagement on a single, interoperable, cloud-based platform.

Description of Services Provided

MIE operates a business unit known as Enterprise Health. This business unit markets health IT applications to large employers, health systems and government entities who operate their own employee health clinics to meet their occupational health and compliance needs.

Enterprise Health monitors the security and availability of the data center infrastructure and the Enterprise Health application.

More information about the Enterprise Health organization and description of services can be found at https://www.enterprisehealth.com.

Components of the System Used to Provide the Services

This report addresses the following five components of the Enterprise Health System, which comprise the boundaries of the system:

- Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
- Software. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).

- Processes and Procedures. The automated and manual procedures.
- Data. Transaction streams, files, databases, tables, and output used or processed by a system.

Infrastructure

Network Zones

The architecture and infrastructure of the Enterprise Health network is designed and maintained in such a way as to ensure that security and availability is sustained. The storage, processing, and retrieval of client data and Enterprise Health corporate data is segregated into different zones.

Internet border

This is our perimeter to the Internet, as well as our first line defense against intruders. A firewall is located here, along with security monitoring and active defense countermeasures.

DMZ

Demilitarized zone shared environment, for our own equipment that does not contain PHI, as well as client owned machines that need internet access.

Guest Wireless

Restricted building wireless access for guests to use while in our office.

Firewall

Our central firewall that protects access across the different zones.

Virtual Machine Cluster

A hosting zone where virtual machines are housed. These machines can be present in any zone, depending on the set configuration in the virtual machine host software.

Production

Servers and networking to support the Enterprise Health system.

MIE Corporate

Medical Informatics' private corporate network and internal services.

Colocation Data Center

Secondary datacenter housing Disaster Recovery equipment and a secondary Internet connection to provide failover capabilities.

Software

The Enterprise Health system is a web-based Software-as-a-Service (SaaS) electronic health record developed and maintained by Enterprise Health's in-house software engineering group. The application is built on the following stack:

- Linux – operating system
- Apache – HTTP server
- MySql (or MariaDB) – relational database management system

- C – programming language

The application supports all major browsers, including Internet Explorer, Edge, Chrome, Firefox, Safari, Opera, as well as other up-to-date browsers.

Enterprise Health is accessible on any mobile device with a browser connected to the Internet. Enterprise Health is mobile optimized and detects the use of a pocket-sized device and optimizes the display of the content for use with these devices.

People

Operations are under the direction of the Chief Executive Officer. Enterprise Health is organized into the following four functional groups:

- Board of Directors

  The Board oversees the organization. The Board is made up of members who are independent from management and meetings are held at least quarterly to review internal control performance. The Enterprise Health Board of Directors is governed by documented bylaws. The Board meets regularly, and the agenda may include Audit Committee updates, the approval of policies, discussion of business operations and financial updates.

  The Enterprise Health Audit Committee is governed by a documented charter. The Audit Committee meets regularly, and the agenda may include managing the external auditor, and reviewing and monitoring audit reports concentrating on financial and information technology controls.

- Corporate Administration

  The CEO is responsible for overseeing strategic financial planning and corporate policy formulation. Administrative responsibilities include oversight of technology resources and service delivery performance and ensuring that these functional areas support the strategic goals and objectives of Enterprise Health. The President coordinates marketing, sales and account management efforts and oversees new service offering planning.

- Information Technology

  The CIO, utilizing departmental supervisors and subject matter technical staff, manages the following functions:

  - Creation and update of Information Security related policies and procedures
  - Technology selection and procurement
  - Systems infrastructure security design

  In addition, the CIO supervises staff responsible for monitoring network security, availability and confidentiality, is an integral member of the computer operations, disaster declaration support, and security and technology maintenance services teams.

- Product Deployment

Product deployment teams are responsible for the stand-up, configuration, training and ongoing support of client environments. This team includes deployment consultants, deployment specialists, and project managers. This area is managed by the Chief Knowledge Officer and the Account Management Director.

- Application Development

  The web application development teams adhere to a rigorous software development life cycle in order to develop quality software that provides an exceptional user experience, has extensive functionality, and safeguards client data based on confidentiality, integrity and availability. This area is managed by the CTO.

- Legal and Regulatory

  Enterprise Health engages with outside counsel for general compliance, legal and legislative requirements. To stay up-to-date with HIPAA regulations, Enterprise Health has engaged with the Tri-State Medical Group, LLC for HIPAA privacy and security support services. The firm assists with documenting HIPAA compliant policies and procedures, trains new hires and all employees annually on HIPAA regulations, and conducts HIPAA security audits.

Processes and Procedures

Enterprise Health has documented policies and procedures to support the operation and controls over the system, available to personnel on MIE's intranet site. Specific examples of the relevant policies and procedures include the following:

- Acceptable Use Policy
  - Two-Factor Authentication Procedure
  - Anti-Virus Procedure
  - Remote Access Standard
- Access Control Policy
  - User Account Provisioning Procedure
- Business Continuity Management Policy
  - Business Continuity Plan
  - Disaster Recovery Plan
  - Business Impact Analysis
- Change Management Policy
  - Software Development Life Cycle
  - Software Quality Process
  - Release Strategy
  - Data Center Change Control Procedure
  - Server Configuration Standard
  - Firewall Standard
- Clean Desk Policy
- Data Center Security Policy
  - Data Center Access Procedure

    - Electronic Media Destruction and Re-Purposing Procedure
- Data Classification Policy
- Encryption Policy
    - Encryption Standard
- Incident Response Policy
    - Incident Response Plan
    - Logging and Monitoring Procedure
- Information Security Awareness
- Information Security Plan
- Information Security Risk Assessment Policy
    - InfoSec Risk Analysis and Management Plan
- Patch Management Policy
    - Vulnerability and Patch Management Procedure
- Password Policy
    - Password Construction Standard
- Physical Security Policy
    - Physical Access Fob Setup Procedure
    - Yubikey Provisioning Procedure
    - Employee Entry/Exit Procedure
    - Visitor Procedure
- Record Retention Policy
    - Record Retention Schedule
- Wireless Communication Policy
    - Wireless Management Procedure

Additional, supporting documentation includes:

- HIPAA Privacy & Security Policies
- HIPAA Privacy Rules
- Enterprise Health Privacy Policy
- EU-US and Swiss-US Privacy Shield Policy
- Master Services Agreement
- Employee Handbook

Data

This component of the system definition is limited to the information used and supported by the system for the purpose of the Enterprise Health System outlined in this description. Enterprise Health is responsible for ensuring the security and availability of data within the Enterprise Health System.

The Enterprise Health application is accessed by users via a secured website using the (TLS) encryption protocol or Virtual Private Network (VPN). User entities are restricted to viewing data within their own unique database and are responsible for administering user access privileges to the web application to authorized personnel. Data is directly input into the electronic health record by the customer via manual input, device interfaces or electronic interface files. Before data is accepted by the application, the input data is inspected and validated to ensure appropriate data characteristics. Records of input data are maintained and available to customers via audit logs.

Data in the application consists of PHI and PII and is stored within either a MySQL or MariaDB relational database management system unique to each customer. The application has robust reporting capabilities, including a data visualization platform. All transactions (data updates, report generations, data viewed and system connections) are logged at a click-level and the logs can be audited by client users with appropriate security privileges. Online support documentation is available to customers regarding data input and output procedures, services and reporting capabilities.

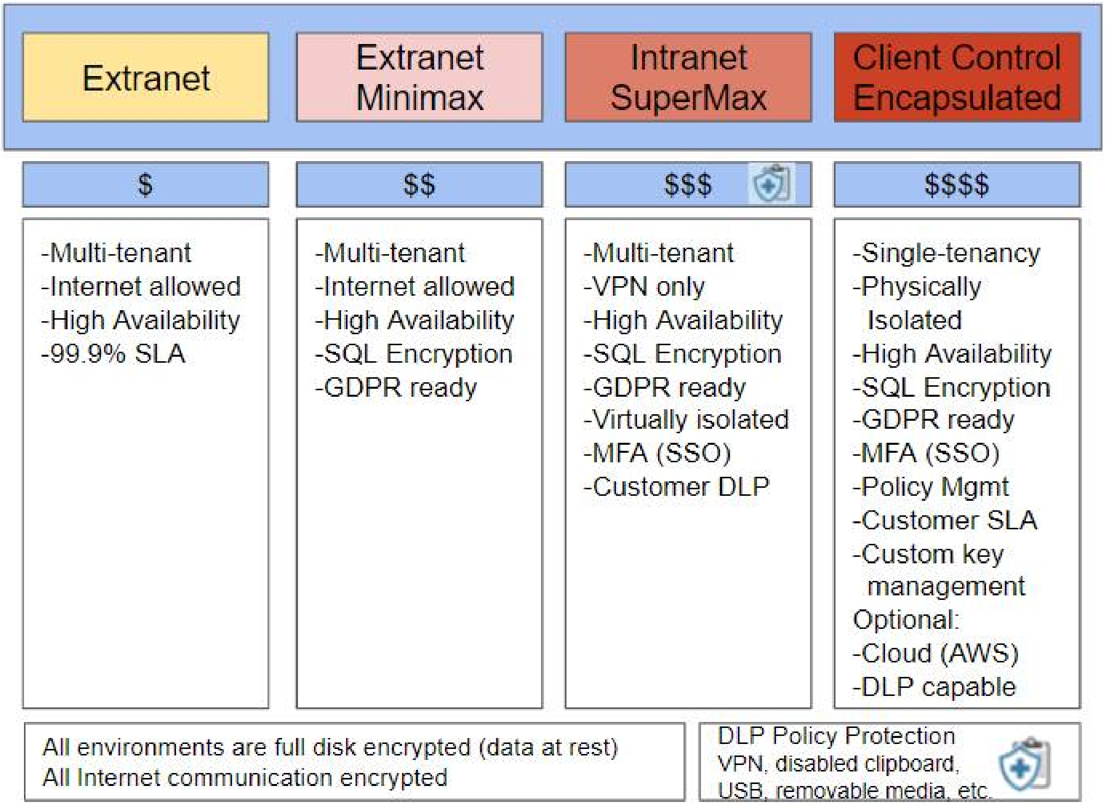
Attachment B

Principal Service Commitments and System Requirements

Enterprise Health designs its processes and procedures related to the Enterprise Health System to meet its objectives. Those objectives are based on the service commitments that Enterprise Health makes to user entities, the laws and regulations that govern the provision of services and the financial, operational, and compliance requirements that Enterprise Health has established for the services. The Enterprise Health services are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act, including relevant regulations, as well as state, federal, and international laws and regulations. Enterprise Health has operational procedures in place to help ensure that customer data security, availability, and confidentiality commitments can be met. Enterprise Health's commitments to user entities are documented and communicated to customers in master service agreements and the service level addendum. Standard security, availability, and confidentiality commitments include, but are not limited to, the following:

- Provide information security measures and system availability.
- Use of encryption technologies to protect customer data both at rest and in transit
- Customer information will not be disclosed to third-parties.

Enterprise Health offers four internal hosting options in order to meet the system objectives of service commitments and system requirements.



Extranet	Extranet Minimax	Intranet SuperMax	Client Control Encapsulated
$	$$	$$$	$$$$
-Multi-tenant -Internet allowed -High Availability -99.9% SLA	-Multi-tenant -Internet allowed -High Availability -SQL Encryption -GDPR ready	-Multi-tenant -VPN only -High Availability -SQL Encryption -GDPR ready -Virtually isolated -MFA (SSO) -Customer DLP	-Single-tenancy -Physically Isolated -High Availability -SQL Encryption -GDPR ready -MFA (SSO) -Policy Mgmt -Customer SLA -Custom key management Optional: -Cloud (AWS) -DLP capable

All environments are full disk encrypted (data at rest)
All Internet communication encrypted

DLP Policy Protection
VPN, disabled clipboard,
USB, removable media, etc.